IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

The United States of America,	:	
	:	
Plaintiff,	:	CIVIL ACTION NO.
v.	:	
	:	
Carahsoft Technology Corp.,	:	
	:	
Defendant.	:	
	:	
	:	
	:	

MEMORANDUM IN SUPPORT OF THE UNITED STATES' PETITION TO ENFORCE CIVIL INVESTIGATIVE DEMAND NO. 22-498

Pursuant to the False Claims Act ("FCA"), 31 U.S.C. § 3733(j), the United States petitions to enforce Civil Investigative Demand ("CID") No. 22-498, which was issued to Carahsoft Technology Corp. (Carahsoft) and served on June 1, 2022. The CID seeks documents and interrogatory responses as part of an ongoing investigation into whether Carahsoft conspired with other companies to rig bids, inflate prices, overcharge, and defraud the Department of Defense (DoD), among other federal government agencies, in selling [redacted] software, cloud storage, and related hardware and services in violation of the FCA, 31 U.S.C. § 3729 *et seq*.

FACTUAL BACKGROUND

A. Carahsoft Technology Corp.

Carahsoft sells several information technology solutions to the federal government. (Decl. ¶¶ 19-26.) For technology solutions manufactured or owned by [redacted] and [redacted] affiliates, Carahsoft sells directly to the government and sells to other resellers, who then sell directly to the federal government. (Decl. ¶¶ 19-21.) This makes Carahsoft both a reseller and distributor

of the [redacted] technology solutions that are within the scope of CID No. 22-498. *See id.* Carahsoft is a large company with over 2,000 employees. (Decl. ¶ 22.) More than two dozen of these employees were involved in the sale of [redacted]-related items to the DoD alone, among the many federal agencies that buy these technology solutions. *Id.* From 2014 to present, which is the time period covered by CID No. 22-498, (*see* Ex. 1-B to Decl. of S. Asiyanbi, Attach. B, at 7), the United States spent over $2 billion on these technology solutions and paid Carahsoft over $990 million dollars directly. (Decl. ¶¶ 25-26.)

B. Issuance and Service of CID No. 22-498

The Department of Justice ("DOJ") issued CID No. 22-498 on May 6, 2022. (*See* Decl. ¶ 3; Ex. 1-B, at 2.) On June 1, 2022, Richard Conway of the law firm of Blank Rome LLP confirmed by email that he has "been authorized by Carahsoft to accept service of the CID." (Decl. ¶ 5.) On the same day, June 1, the United States served CID No. 22-498 on Carahsoft by email to Mr. Conway. (Decl. ¶ 5; Ex. 1-A.)

CID No. 22-498 contains 13 interrogatories and 18 requests for documents. (*See* Ex. 1-B, Attachs. C-D, at 10-13.) The CID was "issued pursuant to the [FCA] in the course of [an FCA] investigation to determine whether" certain companies, "including Carahsoft Technology Corp., conspired to make, made, or caused to be made false claims to the Department of Defense by coordinating the bids, prices, and/or market for [redacted] software, cloud storage, and related hardware and services." (Ex. 1-B, at 1.) CID No. 22-498 seeks communications within Carahsoft, communications between Carahsoft and [redacted] and its affiliates, communications between Carahsoft and other resellers, and communications regarding and between Carahsoft and the government agency customers, as well as the records of the marketing, negotiations, and sales of the technology solutions at issue in this matter. (*See* Ex. 1-B.) Carahsoft has

acknowledged that it has in its possession, custody, or control thousands of documents that are responsive to the CID but that it has failed to produce. (Decl. ¶ 14.) It is also clear from the dealings among the parties that Carahsoft has in its possession, custody, or control considerably more responsive documents and information that it has likewise failed to produce. (Decl. ¶ 15.)

Documents in response to the CID were due 30 days from service or by July 1, 2022. (Decl. ¶ 12.) Interrogatory responses were due 20 days from service or June 21, 2022. (Decl. ¶ 10.) While the CID permits extension of this time period, Carahsoft never sought an extension, nor was one granted to it in writing, as required by the FCA. (Decl. ¶ 18.) It never sought relief from a court using the statutory opportunity to do so. (Decl. ¶ 85); *see* 31 U.S.C. § 3733(j)(2) (allowing a CID recipient to petition the court for redress).

C. Carahsoft Has Refused to Comply with the CID and Has Provided No Reason for its Noncompliance

In over a year, Carahsoft has produced only 2,650 documents in two tranches. (Decl. ¶ 33.) The first tranche was produced in September 2022, and it consisted of 2,647 documents, including an employee's "notebook, various agreements, ESI documents, the ESI BPA, and the Order documents from 2013 through 2019."[1] *Id.* The second tranche was produced in November 2022, and it consisted of three Excel files containing text messages for three of the five employees-custodians that Carahsoft agreed to prioritize. *Id.*

The 2,650 documents that Carahsoft has produced represented only a small fraction of the documents that Carahsoft has confirmed that it has in its possession, custody, or control. (Decl. ¶¶ 34, 37, 52-53, 56.) For example, Carahsoft confirmed in October 2022 that it had prepared

[1] To be sure, Carahsoft sent six production media in the preceding weeks. The documents in the six production media were inaccessible to the United States. Carahsoft later combined these productions into one accessible media in September 2022.

for production "2019 order documents as pages CS17113-CS22074." (Decl. ¶ 53.) That was approximately 4,961 pages of documents. Carahsoft has not produced any of these documents. *Id.*

Carahsoft has not produced a single email communication in this matter, even though it has confirmed having relevant emails, which are expected to constitute the bulk of responsive documents. (Decl. ¶¶ 34.) In September 2022, Carahsoft confirmed that it had identified 5,000 emails that are potentially responsive to the CID. (Decl. ¶ 35.) Carahsoft has not produced any of these emails. *Id.* In January 2023, Carahsoft represented that it was on the verge of "produc[ing] to the Department [of Justice] a large number of emails under the Carahsoft CID in the next week or so." (Decl. ¶ 36.) Carahsoft has not produced any emails at all. *Id.*

Carahsoft used emails to communicate, receive, and transmit transaction records, including but not limited to contracts, agreements, solicitations, bids, quotes, prices, proposals, invoices, purchase orders, and payments. (Decl. ¶¶ 20-21.) While there are a few transaction records in the first production tranche, those records account for only a small fraction of all the transactions in which Carahsoft was involved. (*See* Decl. ¶¶ 33, 53.) Carahsoft has not produced the records of the transactions between Carahsoft and [redacted] affiliates; transactions between Carahsoft and two other resellers, where Carahsoft was the distributor of the technology solutions; and transactions between Carahsoft and various DoD agency customers, where Carahsoft was a direct reseller of the technology solutions. *Id.* In over a year since receiving the CID, Carahsoft has not produced the full set of transaction records (including but not limited to the communications, solicitations, proposals, quotes, bids, award notices, orders, purchase orders, and invoices) for even a single project. (*See* Decl. ¶¶ 27-36, 51-53, 54-63.) Without these records, the United States is unable to reconstruct the factual basis for any

transaction, let alone reconstruct the many transactions and be able to determine whether they reflect the collusive practices and overcharges to the government that the FCA authorizes the government to investigate.

The United States reasonably believes that Carahsoft has in its possession, custody, or control tens of thousands of documents that are responsive to CID No. 22-498. (Decl. ¶¶ 15, 28.) Carahsoft has refused to produce these documents. (Decl. ¶¶ 80-84.) It has even refused to identify the employees-custodians who have these documents, refused to provide information that the United States can use to identify specific custodians and seek their documents from Carahsoft, and refused to inform the United States how many documents it has collected, from whom, and its general process for complying with the CID, all information that could reduce the burden of compliance on Carahsoft if it were legitimately attempting to comply with the CID. (Decl. ¶¶ 37-50.) Instead, Carahsoft has asserted that it considers information regarding its compliance process, including "search terms and a hit list of search terms, to be Work-Product of counsel and not subject to disclosure to DOJ." (Decl. ¶ 32; Ex. 9, at 2.) Carahsoft has not articulated its basis for asserting broadly and indiscriminately that the basic information relating to its compliance or noncompliance with a CID—such as the custodians whose records were collected, the volume of records collected, how the subset of records to be produced were selected, etc.—qualifies for work product protection. *See id.*

Carahsoft's two meager productions do not even comply with the CID instructions for producing electronically stored information ("ESI Instructions"). (Decl. ¶¶ 64-79.) Carahsoft omitted from its productions all but four data fields that are customarily available for electronic documents. (Decl. ¶¶ 71-72.) In order to correct this omission, the United States made several offers for a government technical expert to assist Carahsoft directly. (Decl. ¶¶ 74-78.) The

technical expert even reached out to Carahsoft, through its counsel, to offer his assistance. (Decl. ¶ 76.) Carahsoft rejected all of these offers. (Decl. ¶ 78.) Instead, Carahsoft produced the first tranche of documents with only "four fields," rather than all of the fields available. (Decl. ¶¶ 70-71.) Carahsoft was notified of this omission, but it refused to correct it. (Decl. ¶ 72.) Instead, Mr. Conway has declared that "Carahsoft was under no obligation" to comply with the ESI Instructions. (*See* Decl. ¶ 70.) Carahsoft produced the second tranche without any fields at all. (Decl. ¶ 70; *see* Ex. 1-C, § 2, at 1 ("All applicable metadata/database . . . shall be extracted and provided").) The noncompliance is inexplicable because the United States has had multiple dealings with the law firm representing Carahsoft, and it has been able to produce documents in a manner compliant with the ESI Instructions. (Decl. ¶ 49.)

Finally, CID No. 22-498 contains 13 interrogatory requests. (Decl. ¶10; Ex. 1-B, Attach. C, at 10-11.) "The answers to the interrogatories shall be submitted no later than twenty (20) days from the receipt" of the CID on June 1, 2022, which made the written responses due by June 21, 2022. (Decl. ¶ 10.) To date, Carahsoft has not responded to a single one of the 13 interrogatories. (Decl. ¶ 18.)

ANALYSIS

A "false claims CID is an administrative subpoena and should be enforced if 'the inquiry is within the authority of the agency, the demand is not too indefinite and the information is reasonably relevant to the agency's inquiry.'" *See United States v. Markwood*, 48 F.3d 969, 976 (6th Cir. 1995) (internal quotation marks omitted). The United States' "authority to request records and undertake other investigatory functions is extremely broad," *Santa Fe Energy Prods. Co. v. McCutcheon*, 90 F.3d 409, 414 (10th Cir. 1996) (citing *United States v. Morton Salt Co.*, 338 U.S. 632, 642-43 (1950)), although "a district court's role in enforcing administrative

subpoenas is 'sharply limited.'" *EEOC v. Lockheed Martin Corp.*, 116 F.3d 110, 113 (4th Cir. 1997) (quoting *EEOC v. City of Norfolk Police Dep't*, 45 F.3d 80, 82 (4th Cir. 1995)).

Here, in the Fourth Circuit, "[c]ourts should generally enforce administrative subpoenas where, as an initial matter, the administrative agency shows that (1) it is authorized to make such investigation; (2) it has complied with statutory requirements of due process; and (3) the materials requested are relevant." *EEOC v. American & Efird Mills, Inc.*, 964 F.2d 300, 302-03 (4th Cir. 1992) (citing *Oklahoma Press Publishing Co. v. Walling*, 327 U.S. 186 217-18 (1946)); *EEOC v. City of Norfolk Police Dep't*, 45 F.3d 80, 82 (4th Cir. 1995) (relying on *Efird Mills*); *Lockheed Martin*, 116 F.3d at 113 (relying on *Efird Mills* and *City of Norfolk Police Dep't*); *NLRB v. Carolina Food Processors, Inc.*, 81 F.3d 507, 510 (4th Cir. 1996); *United States v. Clarke*, No. DKC 2003-3440, 2004 U.S. Dist. LEXIS 1657, at *7 (D. Md. Feb. 6, 2004). "The party subpoenaed may then defeat enforcement by showing that the agency's request is excessive or unduly burdensome." *Efird Mills*, 964 F.2d at 303; *Clarke*, 2004 U.S. Dist. LEXIS 1657, at *8. The three requirements for enforcement are met here, as further explained below.

A. DOJ is Authorized to Conduct this Investigation.

The FCA provides civil remedies against "all fraudulent attempts to cause the Government to pay out sums of money." *United States v. Neifert-White Co*., 390 U.S. 228, 233 (1968). The FCA authorizes the DOJ to conduct investigations arising thereunder, and section 3733(a) expressly authorizes the director of the Commercial Litigation Branch, Fraud Section of DOJ (as a "designee" of the Attorney General) to issue CIDs for documents, interrogatories, testimonies, or a combination thereof. *See* 31 U.S.C. § 3733(a)(1); 28 C.F.R. § Ch. 1, Pt. 0, App. Subpt. Y; *see also* A.G. Order No. 3134-2010. As evident on page 2 of the CID issued to Carahsoft, the Director of the Commercial Litigation Branch of the DOJ signed and authorized

CID No. 22-498. (*See* Ex. 1-B, at 2.)

B. CID No. 22-498 Complies with Statutory Requirements of Due Process.

The statutory requirement of due process is met where, as here, there is a process for challenging the issuance or scope of the subpoena. *See* 31 U.S.C. § 3733(j)(2) (allowing a CID recipient to petition the court for redress); *see also EEOC v. Maryland Cup Corp.*, 785 F.2d 471, 476 (4th Cir. 1986) (holding that "EEOC complied with these due process requirements" because underlying statute "offer[s] an internal appeal mechanism" for challenging its subpoena); *Carolina Food Processors*, 81 F.3d at 512 (explaining "that the statutory mechanism for appealing the Board's issuance of subpoenas—namely, that the employer may petition the Board to revoke it—satisfies the requirements of due process."). In compliance with due process, the FCA statute delineates the rights of a CID recipient, the process for challenging the CID, and the timetable for doing so. Carahsoft did not avail itself of these statutory rights and has forfeited their protections.

A recipient of a CID that is issued under the FCA has a legal right to petition a court to modify or set aside the CID. *See* 31 U.S.C. § 3733(j)(2). The statute provides, "Any person who has received a civil investigative demand issued under subsection (a) may file, in the district of the United States . . . a petition for an order of the court to modify or set aside such demand." *Id.* Such petition "must be filed (i) within 20 days after the date of service of the civil investigative demand, or at any time before the return date specified in the demand, whichever date is earlier" or (ii) as "prescribed in writing by any false claims law investigator identified in the demand."

The right to petition a court to modify or set aside CID No. 22-498 satisfies the statutory requirements of due process. Under the circumstances here and the written directions on the CID, Carahsoft had 20 days from June 1, 2022, to "petition for an order . . . to modify or set

aside" the CID. (*See* Ex. 1-B, at 1-2) (relying on 31 U.S.C. § 3733(j)(2)(A)(i)). The statute is not rigid, however. It permits the extension of the time to petition a court to set aside or modify the CID "as may be prescribed in writing by" the FCA investigators. 31 U.S.C. § 3733(j)(2)(A)(ii). Under that provision, Carahsoft could have asked for additional time to comply or to file a petition, but it did neither. (Decl. ¶ 18.)

Ultimately, the availability of these statutory rights satisfies due process and, therefore, meets the requirements for enforcing the CID. *See Maryland Cup Corp.*, 785 F.2d at 476; *Carolina Food Processors*, 81 F.3d at 512. In addition, if Carahsoft had filed a timely petition, it would have failed on the merits because the CID seeks documents and information that are squarely within the scope of the government's investigative authority and permitted by law. Carahsoft would have been unable to demonstrate adequate legal bases for setting aside the CID or modifying it.

C. The Materials Requested by CID No. 22-498 are Relevant.

The Fourth Circuit has explained: "The Supreme Court has characterized the relevancy requirement as 'not especially constraining.' Rather, 'the term 'relevant'' will be 'generously construed' to 'afford[] the Commission access to virtually any material that might cast light on the allegations against the employer.' We determine relevancy 'in terms of the investigation' rather than 'in terms of evidentiary relevance.'" *Lockheed Martin*, 116 F.3d at 113 (internal citations omitted). Indeed, "Courts defer to an agency's own appraisal of what is relevant 'so long as it is not obviously wrong.'" *Id.* (internal quotation marks omitted).

On its face, the CID was issued to investigate whether Carahsoft "conspired to make, made, or caused to be made false claims to the Department of Defense by coordinating bids, prices, and/or market for [redacted] software, cloud storage, and related hardware and services." (Ex.

1-B, at 1); *see United States ex rel. Marcus v. Hess*, 317 U.S. 537, 543-45 (1943) (recognizing that claims submitted under contract obtained through collusive bidding are "false" under the FCA); *United States v. Portsmouth Paving Corp.*, 694 F.2d 312 (4th Cir. 1982) ("The undisputed effect [of collusive bidding] is to force the contracting government entities to pay more for goods and services sought than they would 'had there been free competition in the open market.'") (quoting *Hess*, 317 U.S. at 539 n.1) (internal quotation marks omitted). These claims go to the very essence of the FCA. In furtherance of this investigation, the CID seeks core documents regarding Carahsoft's role and performance as an authorized reseller and distributor of the technology solutions, as well as its interactions with participants in the market for selling and delivering the technology solutions to the United States. It seeks information to determine whether Carahsoft acted alone or whether it acted in a conspiracy to defraud the government. The CID seeks records of payments to determine the damages from any fraud. The CID seeks communications that Carahsoft had internally about these technology solutions; communications with and about the manufacturers; communications with and about the other resellers who acquired quotes from Carahsoft and against whom Carahsoft often submitted bids to the government; communications with and about other third parties who teamed or partnered with Carahsoft to sell these technology solutions; and the transaction history, among other things. (*See* Ex. 1-B, Attach. D, at 11-13.) The CID also seeks 13 interrogatories, including basic information about Carahsoft's agreements and contracts with enumerated market players, custodial information, sales where Carahsoft submitted a direct bid, and communications with other resellers. (*See* Ex. 1-B, Attach. C, at 10-11.) These records and information are manifestly relevant.

In this matter, Carahsoft has in fact conceded that it has documents relevant to the CID.

(Decl. ¶¶ 14, 35, 36, 53.) It has refused to produce these records, despite acknowledging their relevancy. *Id.* And while it has refused to search for and collect other relevant records (e.g., from other employees that it refused to identify as document custodians), Carahsoft has never argued that its failure to search for those records or to comply with the CID was based on any belief that the materials requested were irrelevant to the CID. (Decl. ¶¶ 37-50.)

On multiple occasions, Carahsoft acknowledged that it has in its possession, custody, or control other documents that are relevant to the United States' FCA investigation. (Decl. ¶ 14.) This includes the representation on October 31, 2022 that Carahsoft was "about to provide [approximately 5,000 pages of] reworked 2019 order documents." (Decl. ¶ 53.) Similarly, on January 3, 2023, Carahsoft acknowledged having relevant emails, when it promised to "produce to the Department [of Justice] a large number of emails under the Carahsoft CID in the next week or so." (Decl. ¶ 36.) Despite these admissions, Carahsoft has yet to produce any of these documents. (Decl. ¶¶ 36, 53.)

In addition, the United States has good reason to believe that Carahsoft has other relevant documents that it has refused to identify, collect, and produce, based on the many unproductive exchanges the United States has had with Carahsoft in an attempt to secure compliance with the CID. (Decl. ¶¶ 15, 28.) Carahsoft has refused in these exchanges to identify all custodians with the records that are relevant to the CID, adding only an IT custodian to a list of four that the government provided at the outset. (Decl. ¶¶ 42-45.) Carahsoft never argued that other custodians did not have relevant documents. (*See* Exs. 4 & 9.) To the contrary, it often conceded that they did. *Id.* In one telling example from its November 18, 2022, reply, Carahsoft argued that it did "not agree than [sic] any person who receives only one email or only one text since 2014 is a document custodian per se." (Decl. ¶ 45.) This response misses the point.

Carahsoft's obligation to produce relevant documents does not depend on the volume of documents that an employee-custodian may have. *See* Ex. 1-B, at 1 (requiring Carahsoft to "produce *any and all documents* in your possession, custody, or control responsive to the document requests")) (emphasis added); 31 U.S.C. § 3733(a)(1) (authorizing the Attorney General or a designee to issue a CID to "any person . . . in possession, custody, or control of *any documentary material or information* relevant to a false claims law investigation") (emphasis added). After all, one document or text message can be critical to an investigation, whereas an employee with 10,000 documents may have none that is material at all.

Ultimately, the government and CID recipients can and do consider the volume of documents that a custodian is likely to have in prioritizing among custodians, but that is an accommodation designed to reduce the burden of a CID. (*See* Decl. ¶ 28.) It is not a limit on a CID recipient's obligation to respond fully, meaningfully, and promptly. Here, Carahsoft has refused entirely to identify the employees who are likely to have relevant documents, has refused to describe the process undertaken to collect or preserve potentially relevant documents, and has refused to provide information from which the government can independently identify custodians and make its own assessment as to the documents it needs. (Decl. ¶ 50.) The obvious conclusion to be drawn is that Carahsoft has other relevant responsive documents, in addition to those it admits to having, that is has inexplicably and obstinately failed to produce. (Decl. ¶¶ 15, 28.) Carahsoft's failure to provide these documents and answer the United States' interrogatories is completely at odds with the Fourth Circuit's mandate that "'the term 'relevant'' . . . be '*generously construed*' to 'afford[] the [government] *access to virtually any material that might cast light* on the allegations. . . ." *Lockheed Martin*, 116 F.3d at 113. (emphasis added). The relevancy factor is easily satisfied here.

Finally, Carahsoft's failure to identify custodians creates a high risk of loss of relevant information, including information that, once lost, will be unidentifiable or irretrievable. Messages on a cell phone dissipate over time. Hard copy documents are discarded frequently. Custodians change jobs and, in haste to wrap up, discard materials indiscriminately. It is more difficult to obtain information from former employees. While it is unknown whether any of these things have occurred, we cannot rule out the possibility of the loss of relevant information where, as here, the CID recipient has refused to account for custodians or documents in a reasonable, responsible, or timely manner. For example, Carahsoft's production of text messages is glaringly and inexplicably incomplete for some custodians, and it has not even bothered to produce any text messages for other custodians. (Decl. ¶¶ 54, 58-61.) If, after a year since service of the CID, Carahsoft has not identified other custodians and at least taken an image of the cell phones containing relevant communications, it is very likely that relevant data (including text messages and voicemails) would have been lost. And while it is common practice to issue broad preservation notices, such notices are not always an adequate substitute for engaging in a targeted approach to "identify, collect, and produce any and all data which is responsive to the requests." (*See* Decl. ¶ 62.); *see generally Cognate Bioservices, Inc. v. Smith*, No. WDQ-13-1797, 2014 U.S. Dist. LEXIS 32190, at * 21 (D. Md. Mar. 11, 2014) (recognizing that "[a] federal court may issue preservation orders as part of its inherent authority to manage its own proceedings" and such order may be necessary where, without "'a court order, there is significant risk that relevant evidence will be lost or destroyed – a burden often met by demonstrating that the opposing party has lost or destroyed evidence in the past.'").

D. The CID Requests Are Neither Excessive Nor Unduly Burdensome.

"Once the government has established its prima facie case, the burden shifts to the party challenging the subpoena to demonstrate 'an abuse of process' by showing 'bad faith on the part of the administrative agency in its issuance of the subpoena." *Clarke*, 2004 U.S. Dist. LEXIS 1657, at *8; *see also Efird Mills*, 964 F.2d at 303. Carahsoft cannot meet this burden. CID No. 22-498 seeks documents and information that are definite and identifiable. (*See* Ex. 1-B.) Indeed, Carahsoft has identified many relevant documents and has simply refused to produce them, although the documents that it has acknowledged to date are expected to represent only a fraction of the documents and information required by the CID. (*See* Decl. ¶¶ 35, 36, 53.)

Carahsoft has made a generalized and unpersuasive assertion of undue burden in defense of its hypothetical that an employee with only one document should not be considered a custodian. (*See* Decl. ¶ 45.) This was based on its "belie[f] that [the government's] definition of document custodian is much too broad and would place undue burdens on Carahsoft." *Id.* Not surprisingly, Carahsoft provided no factual basis for the "undue burdens" that would warrant excusing a company the size of Carahsoft from the normal responsibility or burden of responding to an administrative subpoena. (*See* Ex. 9.)

But even assuming without conceding that the requests in CID No. 22-498 are burdensome, courts recognize that "[s]ome burden on subpoenaed parties is to be expected and is necessary in furtherance of the [United States'] legitimate inquiry and the public interest[.]" *FTC v. Texaco, Inc.*, 555 F.2d 862, 882 (D.C. Cir. 1977). Carahsoft is a company with over 2,000 employees that does significant government business. (*See* Decl. ¶ 22.) It received approximately $1 billion from the federal government just for sale of the technology solutions at issue and facilitated up to $1 billion in additional sales. (*See* Decl. ¶¶ 24-26.) It is represented

by a large law firm that can identify and produce documents and information promptly and efficiently. (*See* Decl. ¶¶ 5, 49.) Carahsoft has not articulated how, under the circumstances, it is unduly burdened by a request to provide documents, including some it has already identified but, a year after the service of the CID, has failed to produce.

Moreover, every effort to engage Carahsoft to discuss and potentially negotiate the scope of the requests or priority of documents has been rebuffed or ignored, and the little information Carahsoft has provided about its process makes clear that it is not engaging in a reasonable effort to respond to the CID meaningfully and fully. *See, e.g.*, *Lockheed Martin*, 116 F.3d at 114 ("The efficient search for relevant information is imperative in a case like this, where the [government] must investigate not one or two claims against the company, but nearly two dozens."). It is also incomprehensible why Carahsoft would not produce documents in compliance with the ESI Instructions, especially when it is represented by counsel that does so in other matters before the Fraud Section.

CONCLUSION

For the foregoing reasons, the United States requests that the Court grant its petition for enforcement, order Carahsoft to produce certain documents and information within fourteen (14) days pursuant to CID No. 22-498 and to fully comply with the within twenty (20) days, or such other deadline(s) set by the Court, and that the Court provide any additional relief that the Court deems necessary to correct Carahsoft's noncompliance with a lawful demand.

Respectfully submitted,

BRIAN M. BOYNTON
Principal Deputy Assistant Attorney General

EREK L. BARRON
United States Attorney

MATT HAVEN
Assistant United States Attorney
36 South Charles Street, 4th Floor
Baltimore, MD 21201
(410) 209-4800
Matthew.Haven@usdoj.gov

JAMIE ANN YAVELBERG
SARA McLEAN
SAMSON O. ASIYANBI
VINCENT J. VACCARELLA
Commercial Litigation Branch
United States Department of Justice
175 N Street, N.E., Suite 9.224
Washington, D.C. 20002
(202) 353-1053
(202) 307-0418
Samson.Asiyanbi2@usdoj.gov
Vincent.J.Vaccarella@usdoj.gov